ESET MOBILE SECURITY para Android

Guía del usuario

(desarrollada para las versiones 3.5 y posteriores del producto)

Haga clic aquí para descargar la versión más reciente de este documento



Servicio de atención al cliente: http://support.eset.com/

REV. 30. 1. 2017

Contenido

1. Introducción

ESET Mobile Security es una solución de seguridad completa que protege su dispositivo contra amenazas emergentes y páginas objeto de phishing, filtra llamadas y mensajes no deseados y le permite controlar su dispositivo de manera remota en caso de pérdida o robo.

Entre sus principales funciones se incluyen:

- Antivirus
- Antirrobo
- Anti-Phishing
- Integración con el portal Mi Eset
- Filtro de llamadas y SMS
- Auditoría de seguridad
- Informe de seguridad

1.1 Novedades de la versión 3.5

La versión 3.5 de ESET Mobile Security introduce las siguientes actualizaciones y mejoras:

- Protección proactiva
- Anti-Phishing mejorado
- Informe de seguridad
- Se puede acceder fácilmente a los permisos del sistema desde ESET Mobile Security
- Última ubicación conocida del dispositivo guardada en ESET Antirrobo antes de que la batería del dispositivo se quede sin carga

1.2 Requisitos mínimos del sistema

Para poder instalar ESET Mobile Security, su dispositivo Android debe cumplir con los siguientes requisitos mínimos del sistema:

- Sistema operativo: Android 4 (Ice Cream Sandwich) o posterior
- Resolución de la pantalla táctil: 480 × 800 píxeles mínimo
- CPU: ARM con conjunto de instrucciones ARMv7+, x86 Intel Atom
- RAM: 128 MB
- Espacio libre de almacenamiento interno: 20 MB
- Conexión a Internet

NOTA: No compatible con dispositivos con doble SIM ni con acceso raíz. Antirrobo y Filtro de llamadas y SMS no están disponibles en tabletas que no permiten realizar llamadas ni enviar mensajes.

2. Instalación

ESET Mobile Security puede descargarse en estos canales de distribución:



Google Play: esta aplicación recibe actualizaciones regulares a través de Google Play



Sitio web de ESET: esta aplicación recibe actualizaciones del sistema de actualización de comprobación de versión de ESET



Tienda Apps de Amazon

Para proteger su información personal y los recursos de su dispositivo Android, ESET Mobile Security necesitará acceso a las funciones de su dispositivo y, en algunos casos, tendrá que controlarlas. Para obtener una explicación detallada de cada tipo de permiso y de cómo se utiliza, consulte la tabla de este artículo de la base de conocimiento: http://support.eset.com/kb2711/#PrivacyPolicy
(El artículo no está disponible en todos los idiomas).

2.1 Descargar de Google Play

Abra la aplicación Google Play de su dispositivo Android y busque ESET Mobile Security (o simplemente ESET).

Otra opción es utilizar el vínculo o escanear el código QR que aparece a continuación con su dispositivo móvil y una aplicación de escaneo de códigos QR:



https://play.google.com/store/apps/details?id=com.eset.ems2.gp



2.2 Descargar del sitio web de ESET

La disponibilidad de la versión web varía en función de su región.

1. Descargue el archivo de instalación APK del sitio web de ESET.
2. Asegúrese de que las aplicaciones procedentes de orígenes desconocidos estén autorizadas en su dispositivo. Para ello, pulse el icono del lanzador en la pantalla de inicio de Android (o vaya a Inicio > Menú). Pulse **Ajustes** > **Seguridad**. La casilla de verificación situada junto a **Orígenes desconocidos** debe estar marcada.
3. Abra el archivo desde el área de notificaciones de Android o localícelo con un explorador de archivos. Normalmente, el archivo se guarda en la carpeta Descargas..
4. Pulse **Instalar** y, a continuación, **Abrir**.

2.3 Asistente de inicio

Tras instalar la aplicación, siga los mensajes mostrados en la pantalla del asistente de inicio:

1. Pulse **Idioma** para seleccionar el idioma que quiera utilizar en ESET Mobile Security. Puede modificarse posteriormente en la configuración del programa.

2. Pulse **País** para seleccionar el país en el que reside actualmente.

3. Pulse **Aceptar** para aceptar el Acuerdo de licencia de usuario final.

4. Pulse **Aceptar** en la pantalla **Consentimiento del usuario**. Puede compartirse con ESET información como la ubicación del dispositivo y los sitios web visitados.

Mobile Security

Consentimiento del usuario

Para proporcionarle el máximo nivel de seguridad y funcionalidad podría compartirse cierta información:

- La ubicación del dispositivo, si lo pierde o se lo roban (solo si Antirrobo está activado)
- Sitios web visitados (solo si Antiphishing está activado)

Algunos datos de detección de virus y nombres de aplicaciones se pueden enviar a ESET. Los datos compartidos con ESET son confidenciales y nunca se proporcionarán a terceros.

No acepto | Acepto

5. Pulse **Siguiente** si quiere participar en **ESET Live Grid**. Puede modificarse posteriormente en la configuración del programa. Para leer más información, consulte esta sección.

6. Seleccione **Activar detección** o **No activar detección** para determinar si ESET Mobile Security detectará Aplicaciones potencialmente no deseadas (PUA) y, a continuación, pulse **Siguiente**. Puede modificarse posteriormente en la configuración del programa. Para obtener más información sobre las PUA, consulte esta sección.

7. En el siguiente paso verá una lista de todas las cuentas de correo electrónico disponibles en su dispositivo. Seleccione la cuenta que quiera que ESET utilice para comunicaciones sobre el registro de licencia del producto, información sobre el restablecimiento de la contraseña de seguridad y comunicaciones del servicio de atención al cliente de ESET. Si no hay ninguna cuenta de correo electrónico, pulse **Agregar cuenta** > **Aceptar** > **Existente** para iniciar sesión en su cuenta de correo electrónico existente o pulse **Nueva** para crear una nueva.

8. Pulse **Activar** para activar las funciones Premium del producto o pulse **Omitir** para empezar a utilizar la versión gratuita.

3. Desinstalación

ESET Mobile Security puede desinstalarse con el asistente de desinstalación disponible en el menú principal del programa. Pulse Menú ⋮ > **Configuración** > **Desinstalar**. Se le pedirá que introduzca su contraseña de seguridad.

También puede seguir los pasos que se indican a continuación para desinstalar el producto manualmente:

1. Pulse el icono de inicio en la pantalla de inicio de Android (o vaya a Inicio > Menú) y pulse **Configuración** > **Seguridad** > **Administradores del dispositivo**. Seleccione ESET Mobile Security y pulse **Desactivar**. Pulse **Desbloquear** e introduzca su contraseña de seguridad. Puede omitir este paso si la aplicación ya no está definida como administrador del dispositivo.
2. Vuelva a **Configuración** y pulse **Administrar aplicaciones** > ESET Mobile Security > **Desinstalar**.

4. Activación del producto

ESET Mobile Security tiene tres versiones disponibles:

- Gratuita: las funciones básicas pueden utilizarse de forma gratuita de forma ilimitada
- De prueba: las funciones Premium se activan durante un período de tiempo limitado (30 días de forma predeterminada)
- Premium: las funciones Premium se activan hasta que caduca su licencia

En esta tabla se indica qué funciones están disponibles en las versiones gratuita, de prueba y Premium:

	Gratuita	De prueba y Premium
Antivirus	✔	
Antivirus: análisis automáticos		✔
Actualizaciones automáticas de la base de datos de virus		✔
Antirrobo: comandos por SMS (excepto Eliminación de datos)	✔	
Antirrobo: portal web		✔
Antirrobo: Protección de SIM		✔
Anti-Phishing		✔
Filtro de llamadas y SMS		✔
Auditoría de seguridad		✔
Informe de seguridad	✔	

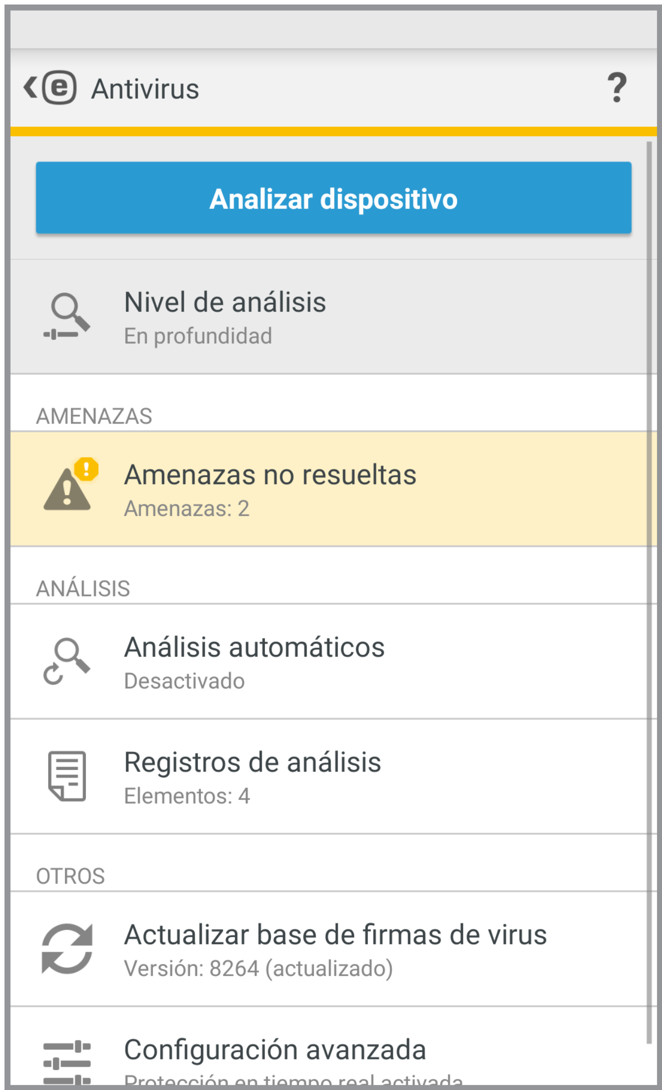
Para activar ESET Mobile Security directamente en su dispositivo Android, pulse Menú ⋮ en la pantalla principal de ESET Mobile Security (o pulse el botón **MENÚ** de su dispositivo) y pulse **Licencia**.

Hay varias formas de activar ESET Mobile Security. La disponibilidad de un método de activación determinado podría variar en función de su país y del medio de distribución (página web de ESET, Google Play, Tienda Apps de Amazon).

- **Comprar la versión Premium**: seleccione esta opción si no tiene licencia y quiere adquirir una a través de Google Play.
- **Introducir una clave de licencia**: seleccione esta opción si ya tiene una clave de licencia. Una clave de licencia es una cadena única con el siguiente formato: XXXX-XXXX-XXXX-XXXX-XXXX, y se utiliza para identificar al propietario de la licencia. Está en el correo electrónico que le ha enviado ESET o en la tarjeta de licencia incluida en la caja que ha adquirido.
- **Activar el periodo de prueba gratuito**: seleccione esta opción si desea evaluar ESET Mobile Security antes de comprar el producto. Solo puede hacerse una vez por cuenta de Google.
- **Tengo un nombre de usuario y una contraseña, ¿qué tengo que hacer?**: seleccione esta opción para convertir su nombre de usuario y su contraseña en una clave de licencia en https://my.eset.com/convert

5. Antivirus

El módulo Antivirus protege su dispositivo de código malicioso mediante el bloqueo de las amenazas y, posteriormente, desinfectándolas.



Analizar dispositivo

Algunos tipos de archivos predefinidos se analizan de forma predeterminada. El análisis del dispositivo revisa la memoria, los procesos en ejecución y las bibliotecas de enlaces dinámicos dependientes, así como los archivos que se encuentran en el almacenamiento interno y en el almacenamiento extraíble. En el apartado Registros de análisis se guardará un archivo de registro con un resumen breve del análisis. Si desea anular un análisis que ya está en curso, pulse ☒.

Nivel de análisis

Es posible elegir entres dos niveles de análisis:

- **Estándar**: el Análisis estándar analizará las aplicaciones instaladas, los archivos DEX (archivos ejecutables del SO Android), los archivos del SO (bibliotecas), los archivos con una profundidad de análisis máxima de tres archivos anidados y el contenido de la tarjeta SD.
- **Exhaustivo**: el Análisis exhaustivo analizará todos los tipos de archivo, sea cual sea su extensión, tanto de la memoria interna como de la tarjeta SD.

Actualizar base de firmas de virus

ESET Mobile Security incluye, de forma predeterminada, una tarea de actualización para garantizar que el programa se actualiza regularmente. Para ejecutar la actualización manualmente, pulse **Actualizar base de firmas de virus**.

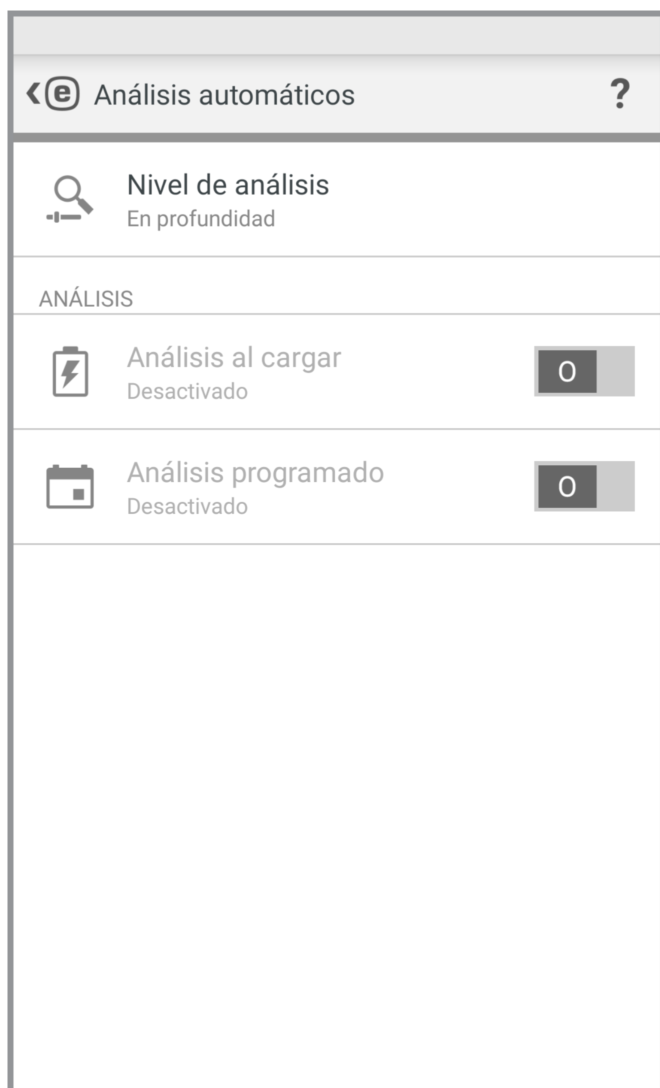
NOTA: para evitar el uso innecesario de ancho de banda, las actualizaciones se emiten a medida que se necesitan cuando se añade una nueva amenaza. Las actualizaciones son gratuitas, aunque su proveedor de servicios móviles podría cobrarle las transferencias de datos.

Para obtener más información sobre análisis, consulte los siguientes vínculos:

- Análisis automáticos
- Registros de análisis
- Configuración avanzada

5.1 Análisis automáticos

Además del análisis del dispositivo iniciado manualmente, ESET Mobile Security ofrece también análisis automáticos.



Nivel de análisis

Es posible elegir entres dos niveles de análisis. Este ajuste se aplicará tanto al Análisis al cargar como al Análisis programado:

- **Estándar**: el Análisis estándar analizará las aplicaciones instaladas, los archivos DEX (archivos ejecutables del SO Android), los archivos del SO (bibliotecas), los archivos con una profundidad de análisis máxima de tres archivos anidados y el contenido de la tarjeta SD.
- **Exhaustivo**: el Análisis exhaustivo analizará todos los tipos de archivo, sea cual sea su extensión, tanto de la memoria interna como de la tarjeta SD.

Análisis al cargar

Cuando se seleccione esta opción, el análisis comenzará automáticamente cuando el dispositivo esté en estado de inactividad, totalmente cargado y conectado a un cargador.

Análisis programado

El Análisis programado le permite programar un análisis automático del dispositivo a una hora predefinida. Para programar un análisis, pulse el conmutador junto a **Análisis programado** y especifique las fechas y horas a las que deba iniciarse el análisis.

5.2 Registros de análisis

La sección Registros de análisis contiene datos completos de cada análisis programado o análisis del dispositivo iniciado manualmente.

En cada registro se incluye la siguiente información:

- Fecha y hora del análisis
- Nivel de análisis (Estándar o Exhaustivo)
- Duración del análisis
- Número de archivos analizados
- Resultado del análisis o errores detectados durante el mismo

Para quitar un registro de la lista, mantenga pulsado el registro para seleccionarlo y pulse Quitar .

5.3 Configuración avanzada

Configuración avanzada ?

PROTECCIÓN

Protección en tiempo real
Activado

ESET LiveGrid®
Activado

Detectar aplicaciones potencialmente no deseadas
Activado

Detectar aplicaciones potencialmente no seguras
Desactivado

ACTUALIZACIÓN

Actualizaciones de base de firmas de virus
Todos los días

Servidor de actualización
Servidor de actualizaciones finales

Protección en tiempo real

El análisis en tiempo real se inicia automáticamente durante el inicio del sistema, y analiza los archivos con los que interactúa. Analiza automáticamente la carpeta *Download* y las aplicaciones instaladas o actualizadas.

ESET Live Grid

Basada en el sistema avanzado de alerta temprana *ThreatSense.Net*, ESET Live Grid está diseñada para proporcionar un nivel adicional de seguridad a su dispositivo. Controla de manera constante los programas y procesos en ejecución del sistema comparándolos con los datos más recientes recopilados de millones de usuarios de ESET de todo el mundo. Además, los análisis se procesan de forma más rápida y precisa a medida que la base de datos de ESET Live Grid va creciendo con el tiempo. Esto nos permite ofrecer una mejor protección proactiva y un análisis más rápido a todos los usuarios de ESET. Se recomienda activar esta función, muchas gracias por su apoyo.

Detectar aplicaciones potencialmente no deseadas

Una aplicación potencialmente no deseada es un programa que contiene software publicitario, instala barras de herramientas, realiza un seguimiento de los resultados de sus búsquedas o tiene otros objetivos poco claros. Existen determinados casos en los que podría creer que las ventajas de una aplicación potencialmente no deseada compensan los riesgos asociados. Este es el motivo que hace que ESET asigne a dichas aplicaciones una categoría de riesgo más baja, en comparación con otros tipos de software malicioso.

Detectar aplicaciones potencialmente no seguras

Existen muchas aplicaciones legítimas que sirven para simplificar la administración de dispositivos en red. Sin embargo, en las manos equivocadas se pueden utilizar con fines maliciosos. Active la opción **Detectar aplicaciones potencialmente no seguras** para supervisar estos tipos de aplicaciones y bloquearlos, si así lo prefiere. Aplicaciones potencialmente no seguras es la clasificación utilizada para el software comercial legítimo. En esta clasificación se incluyen programas como herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones.

Actualizaciones de base de firmas de virus

Esta opción le permite establecer el intervalo de tiempo en el que se descarga automáticamente la base de datos de amenazas. Estas actualizaciones se publican cuando se añade una nueva amenaza a la base de datos. Se recomienda mantener esta opción ajustada en el valor predeterminado (diariamente).

Servidor de actualización

Con esta opción puede optar por actualizar su dispositivo desde el **Servidor de prueba**. Las actualizaciones de prueba han sido sometidas a completas pruebas internas y en breve estarán disponibles para el público en general. Puede beneficiarse mediante el acceso a los métodos y soluciones de detección más recientes. Sin embargo, las actualizaciones de prueba podrían no ser totalmente estables en todo momento. Para ver las versiones de los módulos del programa actuales, pulse Menú ⋮ en la pantalla principal de ESET Mobile Securityy pulse **Acerca de** > **ESET Mobile Security**. Se recomienda que los usuarios básicos dejen la opción **Servidor de lanzamiento** seleccionada de forma predeterminada.

6. Anti-Theft

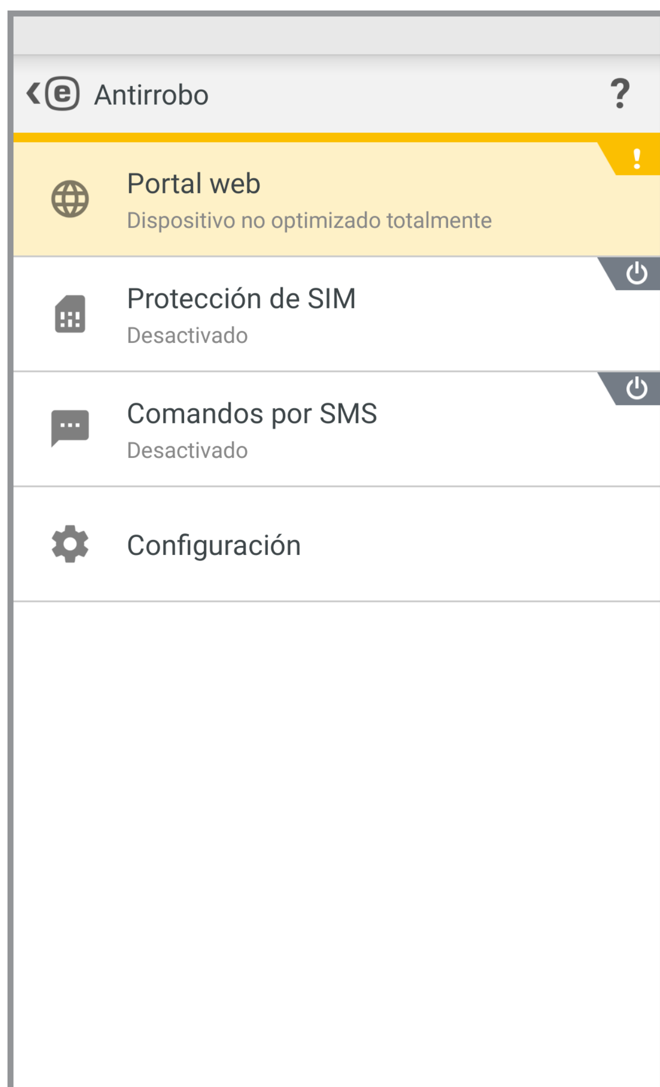
La función **Antirrobo** protege su dispositivo móvil del acceso no autorizado.

Si pierde su dispositivo o alguien se lo roba y sustituye su tarjeta SIM por una nueva (que no es de confianza), ESET Mobile Security bloqueará el dispositivo automáticamente y enviará un SMS de alerta a los números de teléfono que haya definido el usuario. Este mensaje incluirá el número de teléfono de la tarjeta SIM actualmente insertada, el número IMSI (International Mobile Subscriber Identity) y el número de IMEI (International Mobile Equipment Identity) del teléfono. El usuario no autorizado no sabrá que este mensaje se ha enviado, puesto que se eliminará automáticamente de los hilos de mensajes del dispositivo. También puede solicitar las coordenadas GPS del dispositivo móvil perdido o borrar de forma remota todos los datos almacenados en el dispositivo.

NOTA: Algunas funciones de Antirrobo (tarjetas SIM de confianza y comandos de texto por SMS) no están disponibles en los dispositivos que no admiten funciones de mensajería.

6.1 Portal web

La versión 3 de ESET Mobile Security se integra completamente con la protección de ESET Antirrobo a través del portal Mi Eset. Desde el portal podrá controlar la actividad de su dispositivo, bloquear el dispositivo, enviar mensajes personalizados a la persona que localice el dispositivo, activar una potente sirena o eliminar los datos del dispositivo de forma remota.



Para crear un cuenta Mi ESET, pulse **Crear una nueva cuenta** y cumplimente el formulario de registro. Busque el mensaje de confirmación en su bandeja de entrada y haga clic en el enlace que contiene para activar la cuenta. Ya puede administrar las características de seguridad de Antirrobo desde my.eset.com. Si ya tiene una cuenta Mi ESET, pulse **Iniciar sesión** e introduzca su dirección de correo electrónico y su contraseña. Una vez que complete estos pasos, podrá asociar el dispositivo a su cuenta Mi ESET.

Para obtener más instrucciones sobre el uso de funciones de Antirrobo en el portal Mi ESET, consulte la ayuda en línea de Antirrobo o pulse **Ayuda** en la esquina superior derecha de la pantalla.

Última ubicación conocida: esta función guarda la ubicación del dispositivo en ESET Antirrobo antes de que la batería del dispositivo se quede sin carga.

6.1.1 Optimización

La optimización de ESET Anti-Theft consiste en una evaluación técnica medible del estado de seguridad de su dispositivo. La protección con Antirrobo examinará su sistema en relación con los problemas que se enumeran a continuación.

Para cada problema de seguridad, puede pulsar **Cambiar los ajustes** para desplazarse hasta la pantalla en la que puede resolver ese problema específico. Si no desea que ESET Mobile Security informe de un problema, pulse en **Ignorar este problema**.

- **Servicios de ubicación desactivados**: para activarlos, vaya a Ajustes > **Ubicación** y seleccione **Utilizar redes inalámbricas**
- **No se están utilizando los satélites GPS**: acceda a este ajuste en Ajustes > **Ubicación** > **Modo** > **Gran precisión**
- **El bloqueo de pantalla no está protegido**: para proteger su dispositivo con un código de bloqueo de pantalla, una contraseña, un PIN o un patrón, vaya a Ajustes > **Bloquear pantalla** > **Bloqueo de pantalla** y seleccione una de las opciones disponibles. La mayoría de los dispositivos Android ofrecen opciones de desbloqueo con deslizamiento, movimiento, desbloqueo facial, cara y voz, patrón, PIN o contraseña. Si alguien intenta desbloquear el dispositivo con un código incorrecto, ESET Antirrobo le informará de la existencia de una actividad sospechosa en el portal Mi Eset.
- **Los datos móviles no están activados**: acceda a este ajuste en Ajustes > **Conexiones y redes** > **Redes móviles** > **Datos**.
- **Los servicios de Google Play no están presentes**: ESET Antirrobo utiliza los servicios de Google Play para enviar comandos a su dispositivo en tiempo real y mostrar notificaciones push. Si estos servicios están desactivados o no están disponibles en su dispositivo, las funciones de ESET Antirrobo administradas desde Mi Eset estarán limitadas. En estos casos, recomendamos utilizar comandos SMS en vez del portal Mi Eset.

6.1.2 Protección proactiva

Esta función le permite ajustar las advertencias y actividades activadas por el modo Sospechoso, por el que ESET Mobile Security guarda de forma regular la ubicación del dispositivo, las fotos de la cámara y las direcciones IP WiFi. Se puede definir lo siguiente:

- **Activar en intentos de desbloqueo erróneos**: activado predeterminadamente; bloquea el dispositivo cuando se introduce un código de desbloqueo de pantalla incorrecto
- **Número máximo de intentos de desbloqueo erróneos**: número de intentos de desbloqueo erróneo permitidos
- **Tiempo de corrección**: de forma predeterminada, tiene 15 segundos para introducir el código de desbloqueo correcto
- **Guardar fotos en el dispositivo**: guarda las fotos de las cámaras trasera y delantera en la galería del dispositivo y el portal Antirrobo en caso de que se produzca un intento de desbloqueo erróneo o se quite la tarjeta SIM

6.2 Protección de SIM

Para comenzar a utilizar la Protección de SIM, pulse **Antirrobo** > **Protección de SIM** en el menú principal y, a continuación, pulse el conmutador para activar la función. Un sencillo asistente le guiará por el proceso de configuración. También puede acceder a estos pasos con el asistente de configuración de comandos de texto de SMS:

- Escriba una contraseña de seguridad
- Agregue los datos de contacto
- Habilite la protección de desinstalación
- Guarde una tarjeta SIM actual como tarjeta SIM de confianza
- Agregue un amigo de confianza

6.2.1 Tarjetas SIM de confianza

En la sección **Tarjetas SIM de confianza** se muestra la lista de tarjetas SIM aceptadas por ESET Mobile Security. Si inserta una tarjeta SIM que no aparece en esta lista, la pantalla se bloqueará y se enviará un SMS de alerta a los amigos de confianza.

Para agregar una nueva tarjeta SIM, pulse . Escriba el **NOMBRE DE LA TARJETA SIM** (por ejemplo, Casa o Trabajo) y su número IMSI (Identidad Internacional del Abonado a un Móvil). El número IMSI suele aparecer como un número de 15 dígitos impreso en la tarjeta SIM. En algunos casos podría ser más corto.

Para eliminar una tarjeta SIM de la lista, seleccione la tarjeta SIM y pulse .

NOTA: La función Tarjetas SIM de confianza no está disponible en dispositivos CDMA, WCDMA y que solo dispongan de conectividad Wi-Fi.

6.2.2 Amigos de confianza

En la sección Amigos de confianza puede agregar o quitar los números de teléfono de amigos y familiares que podrán:

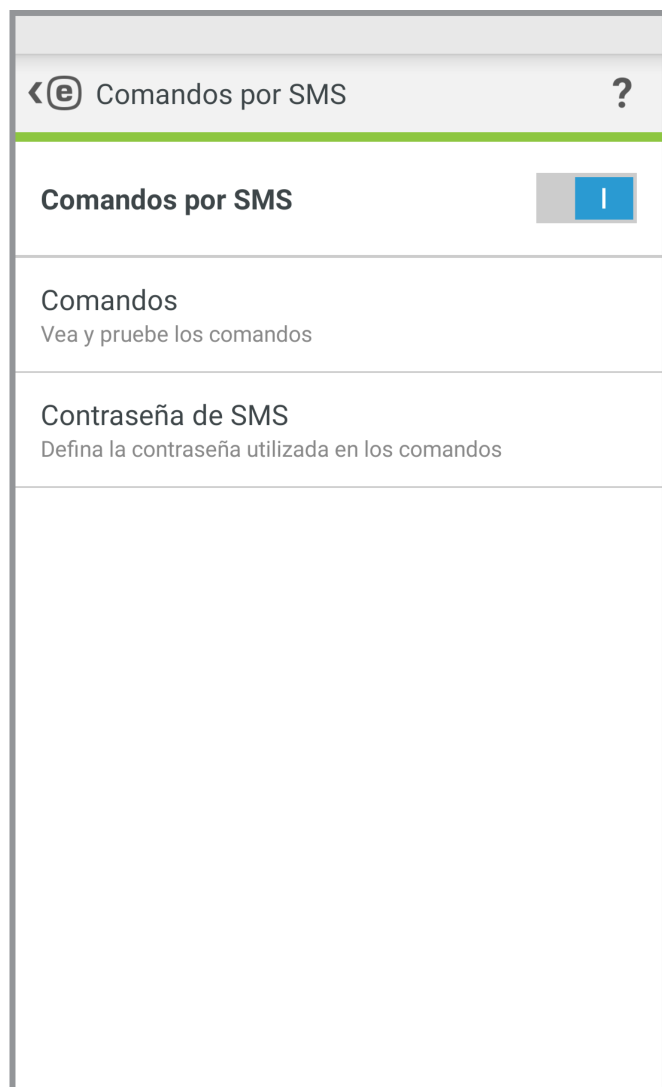
- Recibir un SMS de alerta cuando se detecte una tarjeta SIM no autorizada en su dispositivo
- Restablecer su contraseña de seguridad (si se ha activado la opción **Permitir restablecimiento de contraseña de seguridad remoto** para este contacto)

Para añadir un nuevo amigo de confianza, pulse e introduzca el nombre y el número de teléfono móvil del amigo o pulse para seleccionar un contacto en la lista de contactos de su teléfono. Para quitar un amigo de confianza, seleccione la entrada y pulse Quitar .

Si una entrada de amigo de confianza contiene más de un número de teléfono, el SMS de alerta y el restablecimiento de contraseña funcionarán con todos los números asociados.

NOTA: Si está en el extranjero, introduzca todos los números de teléfono en la lista con el código de marcación internacional seguido del número en cuestión (por ejemplo, +1610100100).

6.3 Comandos por SMS de texto



Para comenzar a utilizar comandos por SMS de texto, pulse **Antirrobo** > **Comandos por SMS de texto** en el menú principal y, a continuación, pulse el conmutador para activar la función. Si ya ha completado los pasos del asistente Protección de SIM, esta configuración solo le pedirá que introduzca un parámetro adicional, la contraseña de SMS. La contraseña de seguridad puede utilizarse para este fin, pero no se recomienda hacerlo, pues la contraseña de SMS podrá verse en pantalla del dispositivo móvil en los mensajes entrantes.

Pueden enviarse los siguientes comandos SMS:

Desbloquear
`eset remote reset`
Envíe este comando desde el dispositivo de un amigo de confianza para desbloquear la pantalla de su dispositivo.

Bloquear
`eset lock contraseña`
Bloqueará el dispositivo: podrá desbloquearlo utilizando la contraseña de seguridad.

Sirena
`eset siren contraseña`
Una potente sirena sonará incluso si el dispositivo está en silencio.

Buscar
`eset find contraseña`
Recibirá un mensaje de texto con las coordenadas GPS del dispositivo de destino y un vínculo a su ubicación en Google Maps. Este dispositivo enviará un nuevo SMS si hay una ubicación más precisa disponible tras determinado período.

Eliminación de datos

`eset wipe contraseña`

Se eliminarán permanentemente del dispositivo todos los contactos, los mensajes, los correos electrónicos, las cuentas, el contenido de la tarjeta SD, las imágenes, la música y los vídeos almacenados en las carpetas predeterminadas. ESET Mobile Security permanecerá instalado en el dispositivo.

NOTA: Aunque los comandos SMS no distinguen entre mayúsculas y minúsculas, es necesario escribir la contraseña tal como se definió en el asistente de configuración de Antirrobo.

6.4 Configuración

En la sección Configuración de Antirrobo, acceda a lo siguiente:

- Contraseña de seguridad
- Datos de contacto

6.4.1 Contraseña de seguridad

Su **Contraseña de seguridad** es necesaria para desbloquear su dispositivo, acceder a Antirrobo, desinstalar ESET Mobile Security o enviar comandos de texto por SMS (si activó esta opción al crear una contraseña de SMS).

Si olvidó la contraseña de seguridad, pruebe con las siguientes opciones:

- Enviar un mensaje de texto desde un número de teléfono móvil de un amigo de confianza a su número. El mensaje debe tener la forma: eset remote reset
- Si su dispositivo está conectado a Internet, solicitar un código de restablecimiento de contraseña pulsando **Correo electrónico** en el dispositivo bloqueado. Se enviará un correo electrónico con el código de verificación a la cuenta de correo electrónico de Google definida durante la instalación. Introduzca el código de verificación y una nueva contraseña en la pantalla bloqueada.
- Restablecer la contraseña desde el portal Mi Eset. Tras iniciar sesión, seleccione su dispositivo, haga clic en **Ajustes** e introduzca una nueva contraseña.
- Si su dispositivo no está conectado a Internet, rellenar el formulario de este artículo de la base de conocimiento.
- Ponerse en contacto con el servicio de atención al cliente de ESET si no puede enviar los datos anteriormente mencionados.

IMPORTANTE: Para crear una contraseña segura más difícil de adivinar, utilice una combinación de letras minúsculas y mayúsculas y números.

6.4.2 Datos de contacto

Si marca su dispositivo como perdido en my.eset.com, la información de **Datos de contacto** se mostrará en la pantalla del dispositivo bloqueado para ayudar al que lo encuentre a ponerse en contacto con usted.

Esta información puede incluir:

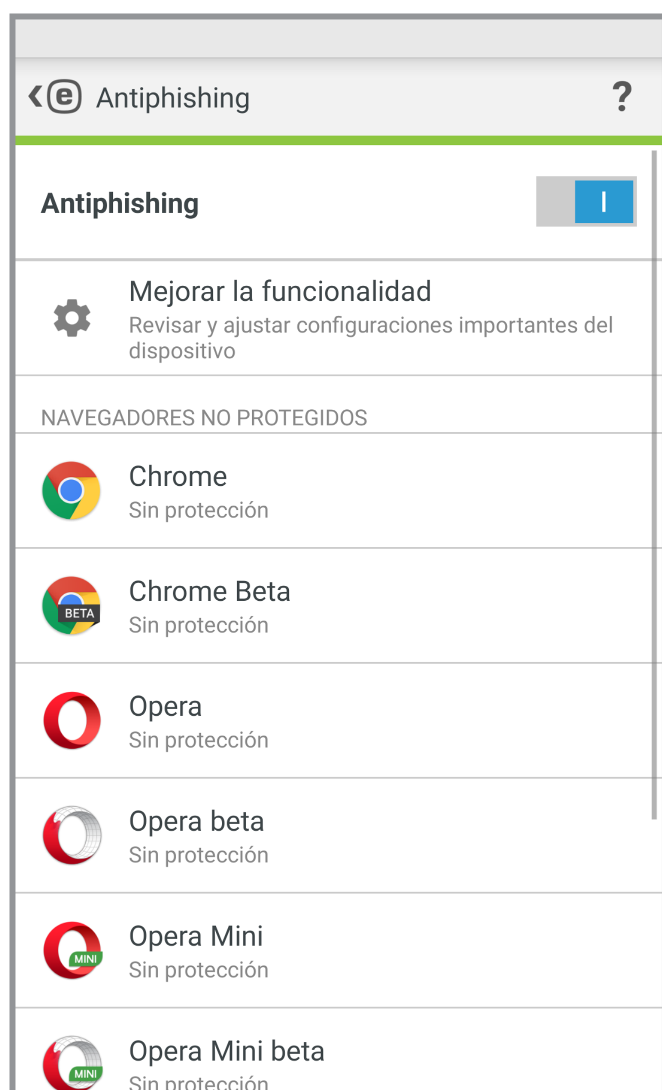
- Su nombre (opcional)
- Número de móvil de respaldo de un familiar o amigo
- Descripción del dispositivo (opcional)
- Dirección de correo electrónico (opcional)

7. Anti-Phishing

El término *phishing* hace referencia a una actividad criminal que utiliza la ingeniería social (la manipulación de usuarios con el fin de obtener información confidencial). El phishing suele utilizarse para acceder a datos confidenciales, como números de cuentas bancarias, números de tarjetas de crédito, números PIN o nombres de usuario y contraseñas.

Se recomienda mantener la función **Anti-Phishing** activada. Se bloquearán todos los posibles ataques de phishing que provengan de sitios web o dominios incluidos en la base de datos de código malicioso de ESET y se mostrará una notificación que le informa del intento de ataque.

Anti-Phishing se integra con la mayoría de navegadores web comunes en el sistema operativo Android (Chrome y navegadores que se incluyen preinstalados de serie en los dispositivos Android, llamados normalmente *Internet* o *Navegador*). El resto de navegadores pueden mostrarse como desprotegidos porque no ofrecen la integración adecuada para el Anti-Phishing. Para utilizar la función Anti-Phishing en su totalidad se recomienda no utilizar navegadores web no compatibles.



Mejorar la funcionalidad: ESET Mobile Security advierte si la Protección antiphishing requiere permisos adicionales que debe conceder el sistema operativo Android. Pulse **Permitir** para abrir la configuración de accesibilidad del sistema y ver las opciones disponibles que ofrecen compatibilidad con más navegadores y activan la protección durante la navegación el modo privado (de incógnito). Si no quiere que este asunto se notifique como problema, pulse **Ignorar este problema (no recomendado)**.

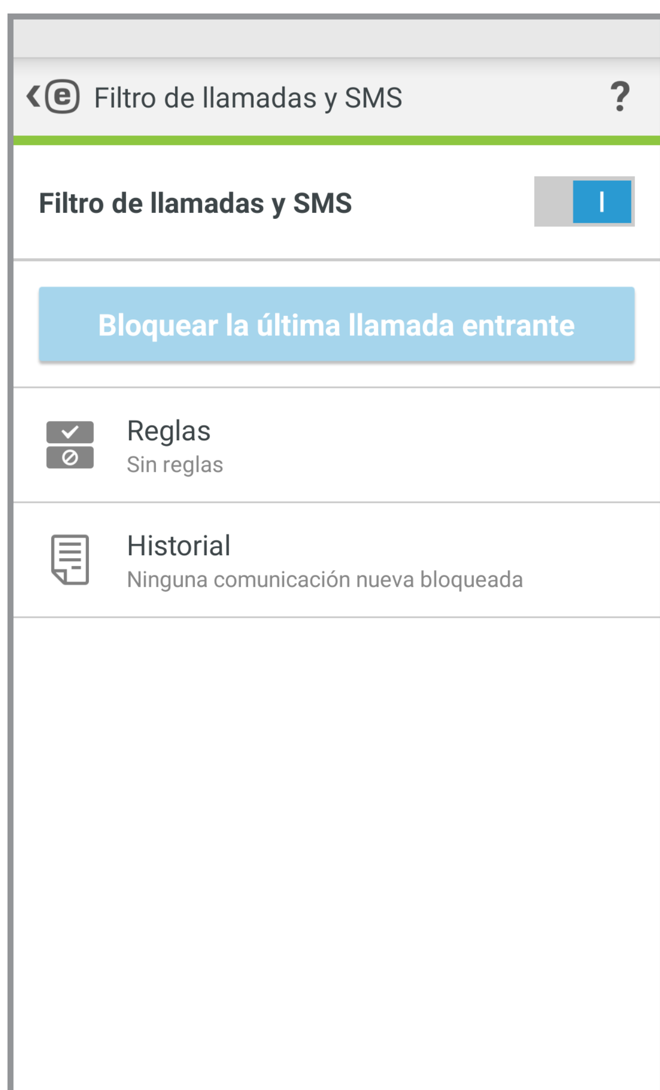
8. Filtro de llamadas y SMS

El **Filtro de llamadas y SMS** bloquea los mensajes SMS/MMS entrantes y las llamadas de voz entrantes/salientes en función de reglas definidas por el usuario.

Los mensajes no solicitados suelen incluir anuncios de proveedores de servicios de telefonía móvil o mensajes de usuarios desconocidos o no especificados. Cuando se bloqueen un mensaje o una llamada de voz entrantes, no se mostrarán notificaciones. Consulte el apartado Historial para buscar llamadas de voz o mensajes que puedan haberse bloqueado por error.

NOTA: El Filtro de llamadas y SMS no funciona en tabletas no compatibles con llamadas y mensajería. El filtrado de SMS/MMS no está disponible en la versión del SO Android 4.4 y posteriores, y se desactivará en aquellos dispositivos en los que Google Hangouts esté configurado como aplicación de SMS principal.

8.1 Reglas



Bloquear la última llamada entrante: pulse para bloquear llamadas entrantes del último número de teléfono. Al hacerlo se creará una nueva regla.

Para crear una nueva regla, pulse **Reglas** > **Agregar regla**. Consulte el siguiente capítulo si desea más información.

Para modificar una regla existente, selecciónela y pulse **Modificar** . Si desea quitar una entrada de la lista **Reglas**, seleccione la entrada y pulse **Quitar** .

8.1.1 Añadir una nueva regla

1. En la sección **Acción**, seleccione **Bloquear** o **Permitir** para especificar el tipo de regla aplicable a llamadas y mensajes.
2. En la sección **Quién**, seleccione una opción para especificar los números de teléfono a los que afectará la regla.
   - **Persona**
   - **Grupo**: ESET Mobile Security reconocerá los grupos de contactos guardados en sus Contactos (por ejemplo, Familia, Amigos o Trabajo).
   - **Todos los números desconocidos** incluirá todos los números de teléfono que no estén guardados en su lista de contactos. Utilice esta opción para bloquear las llamadas de teléfono no deseadas (por ejemplo, las llamadas de empresas que le ofrecen servicios) o para impedir que sus hijos llamen a números desconocidos.
   - **Todos los números conocidos** incluirá todos los números de teléfono guardados en su lista de contactos.
   - **Números ocultos** se aplicará a personas que tengan su número de teléfono oculto intencionadamente a través de la restricción de identificación de llamadas (CLIR).
3. En la sección **Qué**, seleccione el tipo de llamada o texto que debe bloquearse o permitirse:
   llamadas de voz salientes
   llamadas de voz entrantes
   mensajes de texto (SMS) entrantes o
   mensajes multimedia (MMS) entrantes
4. En la sección **Cuándo**, seleccione **Siempre** o **Personalizar** para especificar el intervalo de tiempo y los días de la semana que estará en vigor la regla. De forma predeterminada se seleccionan sábado y domingo.

NOTA: Si está en el extranjero, introduzca todos los números de teléfono en la lista con el código de marcación internacional seguido del número en cuestión (por ejemplo, +1610100100).

8.2 Historial

En el apartado **Historial** se muestra el registro de todas las llamadas y los mensajes bloqueados por el Filtro de llamadas y SMS. Cada registro incluye el nombre del evento, el número de teléfono correspondiente, la fecha y la hora del suceso. Los registros de mensajes SMS y MMS contienen también el cuerpo del mensaje.

Si desea quitar una entrada de la lista, selecciónela y pulse Quitar .

9. Auditoría de seguridad

La Auditoría de seguridad le ayuda a supervisar y cambiar ajustes importantes del dispositivo y revisar los permisos de las aplicaciones instaladas para evitar riesgos de seguridad.

Para activar o desactivar la Auditoría de seguridad y sus componentes específicos, pulse .

- Supervisión de dispositivo
- Auditoría de aplicación

9.1 Supervisión de dispositivo

En la sección **Supervisión de dispositivo**, defina qué componentes del dispositivo supervisará ESET Mobile Security.

Pulse cada opción para ver su descripción detallada y su estado actual. En las opciones **Orígenes desconocidos** y **Modo de depuración**, pulse **Abrir configuración** para cambiar los ajustes en Ajustes del sistema operativo Android.

Supervisión del dispositivo

Wi-Fi
Avisar al conectar a una red abierta

Memoria
Avisar cuando haya poca memoria

Itinerancia de datos
Avisar al detectar itinerancia de datos

Itinerancia de llamadas
Avisar al conectar a una red de itinerancia

Orígenes desconocidos
Avisar cuando esté permitida la instalación desde orígenes desconocidos

Modo de depuración
Avisar cuando esté activado

9.2 Auditoría de aplicación

La Auditoría de aplicaciones realiza una auditoría de las aplicaciones instaladas en el dispositivo que podrían tener acceso a servicios que le suponen un gasto, que controlan su ubicación o que leen su información de identificación, sus contactos o sus mensajes de texto. ESET Mobile Security ofrece una auditoría de dichas aplicaciones clasificadas en categorías. Pulse las diferentes categorías para ver una descripción detallada. Pulse una aplicación para ver sus detalles de permisos.

Auditoría de aplicaciones

Administrador del dispositivo
No hay aplicaciones

Utilizar servicios de pago
Aplicaciones nuevas: 6

Rastrear ubicación
Aplicaciones nuevas: 16

Leer información de identidad
Aplicaciones nuevas: 10

Leer datos personales
Aplicaciones nuevas: 5

Soporte de grabación
Aplicaciones nuevas: 12

Acceso a los mensajes
Aplicaciones nuevas: 3

Acceso a los contactos
Aplicaciones nuevas: 9

10. Informe de seguridad



Informe de seguridad contiene una completa visión global de cada módulo del programa y sus respectivos estado y estadísticas. También puede activar los módulos que no se encuentren en uso desde la pantalla Informe de seguridad. Cada sección del módulo del programa contiene la información que se indica a continuación.

Antivirus:

- Aplicaciones instaladas
- Aplicaciones actualizadas
- Aplicaciones analizadas
- Amenazas detectadas
- Actualizaciones de base de firmas de virus

Antirrobo

Anti-Phishing:

- Sitios web analizados
- Amenazas detectadas

Filtro de llamadas y SMS:

- Llamadas salientes
- Llamadas recibidas
- Llamadas bloqueadas

Auditoría de seguridad:

- Alertas de roaming
- Avisos de Wi-Fi abierto

Active la opción **Notificación de informe mensual** para mostrar un breve mensaje en la barra de notificaciones de Android. Pulse la notificación para abrir la ventana **Informe de seguridad**.

11. Configuración

Para acceder a la configuración del programa, pulse Menú ⋮ en la pantalla principal de ESET Mobile Security (o pulse el botón Menú de su dispositivo) y pulse **Configuración**.

Idioma

De forma predeterminada, ESET Mobile Security se instala en el idioma establecido como valor predeterminado del sistema en su dispositivo (en la configuración de **Teclado e idioma** del SO Android). Si desea cambiar el idioma de la interfaz de usuario de la aplicación, pulse Idioma y seleccione el idioma que quiera.

Notificación permanente

El icono de ESET Mobile Security se mostrará en la esquina superior izquierda de la pantalla (barra de estado de Android). Si no quiere que este icono se muestre, cancele la selección de **Notificación permanente** y pulse **Desactivar**.

Ofertas especiales

Recibirá las noticias en el producto y las últimas ofertas de ESET.

Actualización

Para disfrutar de la máxima protección es importante usar la versión más reciente de ESET Mobile Security. Pulse **Actualizar** para ver si hay una versión más reciente disponible para su descarga desde el sitio web de ESET. Esta opción no está disponible si se realizó la descarga de ESET Mobile Security desde Google Play; en este caso, la actualización del producto se realiza desde Google Play.

Asistente de

Si ejecuta el asistente de desinstalación, ESET Mobile Security se quitará del dispositivo de forma permanente. Si se activó la protección de desinstalación, se le solicitará que introduzca la contraseña de seguridad. Para desinstalar el producto manualmente, siga los pasos que se describen en esta sección.

12. Atención al cliente

Los especialistas de atención al cliente de ESET están disponibles para prestar ayuda administrativa y ofrecer soporte técnico relacionado con ESET Mobile Security y con cualquier otro producto de ESET.

Para ponerse en contacto con el servicio de atención al cliente de ESET, utilice este vínculo.

Si desea enviar una solicitud de soporte técnico directamente desde su dispositivo, pulse Menú ⋮ en la pantalla principal de ESET Mobile Security (o pulse el botón Menú de su dispositivo), pulse **Atención al cliente** > **Atención al cliente** y cumplimente los campos obligatorios. ESET Mobile Security incluye funciones de registro avanzadas para ayudarle a diagnosticar posibles problemas técnicos. Para proporcionar a ESET un registro detallado de la aplicación, asegúrese de que está seleccionada la opción **Enviar registro de la aplicación** (predeterminada). Pulse **Enviar** para enviar su solicitud. Un especialista del servicio de atención al cliente de ESET se pondrá en contacto con usted en la dirección de correo electrónico proporcionada.